This is a previous version of the article published in Linear and Multilinear Algebra. 2017, 65(12): 2424-2431. doi:10.1080/03081087.2016.1275507

A construction of primitive polynomials over finite fields

Sara D. Cardell[a] and Joan-Josep Climent[b]

[a] Instituto de Matemática, Estatística e Computação Científica,
Universidade Estadual de Campinas, Brazil.
[b] Departament de Matemàtiques
Universitat d'Alacant, Spain.

Abstract

In this work, a new construction based on companion matrices of primitive polynomials is provided. Given two primitive polynomials over the finite fields $\mathbb{F}_q$ and $\mathbb{F}_{q^b}$, we construct a ring isomorphism that transforms the companion matrix of the primitive polynomial over $\mathbb{F}_{q^b}$ into a matrix with elements in $\mathbb{F}_q$ whose characteristic polynomial is another primitive polynomial over $\mathbb{F}_q$.

Keywords: Primitive polynomial, companion matrix, ring isomorphism, finite field.

AMS Subject Classification:12E05

1 Introduction

Primitive polynomials have been extensively studied because of their important applications (see, for example, [1]). They are widely used in cryptographic applications such that pseudo-random sequence generation. For example, every linear feedback shift register (LFSR) with maximum period is built from a primitive polynomial [2]. Many other sequence generators are based on primitive polynomials, for example, the shrinking generators (see [3, 4, 5]).

On the other hand, linear block codes that achieve equality in the Singleton bound are called maximum distance separable codes (MDS codes) [6]. The companion matrices of primitive polynomials are used to construct maximum distance separable (MDS) codes [7]. MDS codes are an important class of block codes since, for a fixed length and dimension, they have the greatest error correcting and detecting capabilities. These codes have been under study extensively due to their error correcting ability, they are, for instance, widely used in storage systems to protect data against erasures [8].

Various tables of primitive polynomials over finite fields were presented in the technical literature [9, 10]. Primitive polynomials over the binary field, $\mathbb{F}_2$, have received particular attention, due to their use in the generation of linear recurring sequences widely employed in testing, coding theory, cryptography, communication systems, and many other areas of electrical engineering [11, 12, 13]. There have appeared a number of recent results about primitive polynomials, for instace, dealing with the existence of primitive polynomials with prescribed coefficients [14, 15, 16].

In some applications, we need primitive polynomials with some special properties, and so it is very important to know whether for any given q and b there exists a primitive polynomial of degree b over the Galois field $\mathbb{F}_q$ which satisfies certain conditions [17, 18, 10]. For this purpose, in this work, we present a ring isomorphism that combines two companion matrices of two given primitive polynomials and provides a new matrix whose characteristic polynomial is also primitive.

This paper is organized as follows: In Section 2 some basic concepts and definitions are given. In Section 3,

the main construction of this work is presented. Finally, the paper comes to an end in Section 4 with some conclusions.

2 Preliminaries

In this section, we recall some concepts that are well-known and can be found in reference [19].

Let $\mathbb{F}_q$ be the Galois field of q elements. A generator of the cyclic group $\mathbb{F}_q^*$ is called a **primitive element** of $\mathbb{F}_q$.

A polynomial $A(\mathsf{x}) \in \mathbb{F}_q[x]$ of degree $m \geq 1$ is called **primitive** over $\mathbb{F}_q$ if it is the minimal polynomial over $\mathbb{F}_q$ of a primitive element of $\mathbb{F}_{q^m}$. Thus, a primitive polynomial over $\mathbb{F}_q$ of degree m may be described as a monic polynomial that is irreducible over $\mathbb{F}_q$ and has a root $\alpha \in \mathbb{F}_{q^m}$ that generates the multiplicative group of $\mathbb{F}_{q^m}$.

The **companion matrix** of a monic polynomial $A(\mathsf{x}) = a_0 + a_1\mathsf{x} + a_2\mathsf{x}^2 + \cdots + a_{m-1}\mathsf{x}^{m-1} + \mathsf{x}^m \in \mathbb{F}_q[\mathsf{x}]$ is given by the $m \times m$ matrix

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & -a_{m-2} \\ 0 & 0 & \cdots & 1 & -a_{m-1} \end{bmatrix}.$$

Some authors define the companion matrix of $A(x)$ as $\mathbf{A}^T$.

Example 1: The polynomial $p(x) = 1+\mathsf{x}+\mathsf{x}^3 \in \mathbb{F}_2[\mathsf{x}]$ is a primitive polynomial over $\mathbb{F}_2$ with companion matrix:

$$P = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

A root $\alpha \in \mathbb{F}_{q^m}$ of $p(\mathsf{x})$ generates the multiplicative group of $\mathbb{F}_{2^3}$ in the following way:

$$\begin{aligned} \mathbb{F}_{2^3} &= \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\} \\ &= \{0, 1, \alpha, \alpha^2, 1+\alpha, \alpha+\alpha^2, 1+\alpha+\alpha^2, 1+\alpha^2\} \end{aligned}$$ ■

3 Construction

We can use a primitive polynomial $U(\mathsf{x})$ of degree m in order to construct $\mathbb{F}_{q^m}$, the Galois field of q^m elements [19]. Thus,

$$\begin{aligned} \mathbb{F}_{q^m} &\approx \mathbb{F}_q[\mathsf{x}]/\langle U(\mathsf{x})\rangle \\ &= \left\{a_0 + a_1\mathsf{x} + \cdots + a_{m-2}\mathsf{x}^{m-2} + a_{m-1}\mathsf{x}^{m-1} \mid a_i \in \mathbb{F}_q, i = 0, 1, \ldots, m-1\right\} \end{aligned}$$

and addition and multiplication in $\mathbb{F}_{q^m}$ are the usual in $\mathbb{F}_q[\mathsf{x}]$, but reducing modulo $U(\mathsf{x})$.

Another way to see the elements in $\mathbb{F}_{q^m}$ is as vectors in $\mathbb{F}_q^m$, that is,

$$\mathbb{F}_{q^m} = \{(a_0, a_1, \ldots, a_{m-2}, a_{m-1}) \mid a_i \in \mathbb{F}_q, i = 0, 1, \ldots, m-1\}.$$

Moreover, if $\alpha \in \mathbb{F}_{q^m}$ is a root of $U(\mathsf{x})$, then α is a primitive element of $\mathbb{F}_{q^m}^*$ and we can write

$$\mathbb{F}_{q^m} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q^m-2}\}.$$

We can also see the elements in $\mathbb{F}_{q^m}$ as matrices. For this purpose, we consider the companion matrix $\mathbf{U}$ of the primitive polynomial $U(\mathsf{x})$. In this case, it is well-known that $\mathbb{F}_q[\mathbf{U}] = \{F(\mathbf{U}) \mid F(\mathsf{x}) \in \mathbb{F}_q[\mathsf{x}]\}$ is a field which is isomorphic to $\mathbb{F}_{q^m}$ (see, for example [19]). Now, we can consider the field isomorphism

$$\begin{array}{ccc} \psi : \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_q[\mathbf{U}] \\ \psi(\alpha) & \mapsto & \mathbf{U} \end{array} \tag{1}$$

where $\alpha \in \mathbb{F}_{q^m}$ is a primitive element [7, 19]. Then we can write

$$\mathbb{F}_{q^m} = \left\{\mathbf{O}, \mathbf{I}, \mathbf{U}, \mathbf{U}^2, \ldots, \mathbf{U}^{q^m-2}\right\}.$$

This isomorphism can be extended to the following ring isomorphism (see [7]):

$$\begin{array}{ccc} \Psi : \mathrm{Mat}_{t\times s}(\mathbb{F}_{q^m}) & \longrightarrow & \mathrm{Mat}_{t\times s}(\mathbb{F}_q[\mathbf{U}]) \\ \mathbf{A} = [a_{i,j}] & \mapsto & \Psi(\mathbf{A}) = [\psi(a_{i,j})] \end{array} \tag{2}$$

Next theorem shows how to use this ring isomorphism in order to construct primitive polynomials with coefficients in $\mathbb{F}_q$ using primitive polynomials with coefficients in $\mathbb{F}_{q^m}$.

Theorem 3.1: *Let $\mathbf{V}$ be the companion matrix of a primitive polynomial $V(\mathsf{x}) \in \mathbb{F}_{q^m}[\mathsf{x}]$ of degree r, and let Ψ be the ring isomorphism given in expression (2). Then, the characteristic polynomial $C(\mathsf{x}) = \det(\mathsf{x}\mathbf{I} - \Psi(\mathbf{V})) \in \mathbb{F}_q[\mathsf{x}]$ of the matrix $\Psi(\mathbf{V})$ is a primitive polynomial of degree rm.*

PROOF: Assume that $V(\mathsf{x}) = v_0 + v_1\mathsf{x} + \cdots + v_{r-1}\mathsf{x}^{r-1} + \mathsf{x}^r \in \mathbb{F}_{q^m}[\mathsf{x}]$ and let

$$\mathbf{V} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -v_0 \\ 1 & 0 & 0 & \cdots & 0 & -v_1 \\ 0 & 1 & 0 & \cdots & 0 & -v_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -v_{r-2} \\ 0 & 0 & 0 & \cdots & 1 & -v_{r-1} \end{bmatrix}$$

be its companion matrix. We have to prove that the characteristic polynomial of the matrix

$$\Psi(\mathbf{V}) = \begin{bmatrix} \mathbf{O} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & -\psi(v_0) \\ \mathbf{I}_m & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & -\psi(v_1) \\ \mathbf{O} & \mathbf{I}_m & \mathbf{O} & \cdots & \mathbf{O} & -\psi(v_2) \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & -\psi(v_{r-2}) \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{I}_m & -\psi(v_{r-1}) \end{bmatrix} \tag{3}$$

is a primitive polynomial in $\mathbb{F}_q[\mathsf{x}]$ with degree rm.

On one hand, we know hat the matrix $\Psi(\mathbf{V})$ has size $rm \times rm$, so the characteristic polynomial $C(\mathsf{x}) = \det(\mathsf{x}\mathbf{I}_{rm} - \Psi(\mathbf{V}))$ must have degree rm.

On the other hand, we also know that the polynomial $C(\mathsf{x})$ is a primitive polynomial if and only if all the powers $\Psi(\mathbf{V})^i$, for $i = 1, 2, \ldots, q^{rm} - 1$ are pairwise different [20]. First of all, it is clear that $\Psi(\mathbf{V})^i \in \mathrm{Mat}_{rm\times rm}(\mathbb{F}_q)$, for $i = 1, 2, \ldots, q^{rm} - 1$. Suppose now that $\Psi(\mathbf{V})^i = \Psi(\mathbf{V})^j$, for some $i, j \in \{1, 2, \ldots, q^{rm} - 1\}$. Since Ψ is a ring isomorphism, we have that

$$\mathbf{V}^i = \mathbf{V}^j \quad \text{in} \quad \mathrm{Mat}_{r\times r}(\mathbb{F}_{q^m}).$$

Moreover, since $\mathbf{V}$ is the companion matrix of a primitive polynomial in $\mathbb{F}_{q^m}[\mathsf{x}]$, we have that $\mathbb{F}_{q^{rm}} \approx \mathbb{F}_{q^m}[\mathbf{V}]$ and, therefore

$$i - j \equiv 0 \pmod{(q^m)^r - 1},$$

and consequently $i = j$ from the choice of i and j. □

The next example illustrates all the work made in this construction.

Example 2: Consider the primitive polynomial $U(\mathsf{x}) = 1 + \mathsf{x} + \mathsf{x}^2 \in \mathbb{F}_2[\mathsf{x}]$. We can use this polynomial to construct the Galois field $\mathbb{F}_{2^2}$ of 4 elements. Thus,

$$\mathbb{F}_{2^2} \approx \mathbb{F}_2[\mathsf{x}]/\langle U(\mathsf{x})\rangle = \{a_1\mathsf{x} + a_0 \mid a_0, a_1 \in \mathbb{F}_2\}$$

and the addition and multiplication in $\mathbb{F}_{2^2}$ are the usual in $\mathbb{F}_2[\mathsf{x}]$ but modulo $U(\mathsf{x})$.

Another way to see the elements in $\mathbb{F}_{2^2}$ is as vectors in $\mathbb{F}_2^2$, that is

$$\mathbb{F}_{2^2} = \{(0,0), (0,1), (1,0), (1,1)\}$$

or,

$$\mathbb{F}_{2^2} = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}\}$$

with the operations given by the tables:

$+$	**0**	**1**	**2**	**3**
0	**0**	**1**	**2**	**3**
1	**1**	**0**	**3**	**2**
2	**2**	**3**	**0**	**1**
3	**3**	**2**	**1**	**0**

$\cdot$	**0**	**1**	**2**	**3**
0	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**
2	**0**	**2**	**3**	**1**
3	**0**	**3**	**1**	**2**

Here **0**, **1**, **2** and **3** are the binary expansion of 0, 1, 2 and 3 respectively.

Another way to see the elements in $\mathbb{F}_{2^2}$ is as matrices. For this purpose, we consider the companion matrix $\mathbf{U}$ of $U(\mathsf{x})$, that is,

$$\mathbf{U} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

and, since $U(\mathsf{x})$ is a primitive polynomial, we know that

$$\mathbb{F}_{2^2} \approx \mathbb{F}_2[\mathbf{U}] = \{\mathbf{O}, \mathbf{I}, \mathbf{U}, \mathbf{U} + \mathbf{I}\} = \{\mathbf{O}, \mathbf{I}, \mathbf{U}, \mathbf{U}^2\}.$$

Now, as we saw before, given a primitive element, for example $\alpha = \mathbf{3} \in \mathbb{F}_{2^2}$, we can construct the map $\psi : \mathbb{F}_{2^2} \longrightarrow \mathbb{F}_2[\mathbf{U}]$ such that $\psi(\mathbf{3}) = \mathbf{U}$ is a field isomorphism. It is possible to construct the ring isomorphism $\Psi : \mathrm{Mat}_{t\times s}(\mathbb{F}_{2^2}) \longrightarrow \mathrm{Mat}_{t\times s}(\mathbb{F}_2[\mathbf{U}])$, such that $\Psi(\mathbf{A}) = [\psi(a_{ij})]$, for $\mathbf{A} = [a_{ij}] \in \mathrm{Mat}_{t\times s}(\mathbb{F}_{2^2})$.

Now, consider the primitive polynomial $V(\mathsf{x}) = \mathbf{3} + \mathbf{2}\mathsf{x} + \mathsf{x}^2 + \mathsf{x}^3 \in \mathbb{F}_{2^2}[\mathsf{x}]$ whose companion matrix is

$$\mathbf{V} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{3} \\ \mathbf{1} & \mathbf{0} & \mathbf{2} \\ \mathbf{0} & \mathbf{1} & \mathbf{1} \end{bmatrix}.$$

Then,

$$\Psi(\mathbf{V}) = \begin{bmatrix} \mathbf{O} & \mathbf{O} & \mathbf{V} \\ \mathbf{I} & \mathbf{O} & \mathbf{V}^2 \\ \mathbf{O} & \mathbf{I} & \mathbf{I} \end{bmatrix} = \left[\begin{array}{cc:cc:cc} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ \hdashline 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ \hdashline 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right]$$

and by Theorem 3.1 the characteristic polynomial

$$C(\mathsf{x}) = \det\left(\mathsf{x}\mathbf{I} - \Psi(\mathbf{V})\right) = 1 + \mathsf{x} + \mathsf{x}^6$$

of matrix $\Psi(\mathbf{V})$ is a primitive polynomial with coefficients in $\mathbb{F}_2$ and degree 6.

Summarizing, with a polynomial of degree 3 over $\mathbb{F}_{2^2}[\mathsf{x}]$ and a polynomial of degree 2 over $\mathbb{F}_2[\mathsf{x}]$ we found a polynomial $C(\mathsf{x})$ of degree 6 over $\mathbb{F}_2[\mathsf{x}]$. Now, if we had a polynomial of degree t over $\mathbb{F}_{2^6}$ and $C(\mathsf{x})$, we could find a primitive polynomial of degree $6t$ over $\mathbb{F}_2[\mathsf{x}]$. ■

In order to reduce the complexity of the computation of the determinant considered in the previous theorem, we introduce the following result.

Corollary 3.2: *Let* $\mathbf{V}$ *be the companion matrix of a primitive polynomial* $V(\mathsf{x}) = v_0 + v_1\mathsf{x} + \cdots + v_{r-1}\mathsf{x}^{r-1} + \mathsf{x}^r \in \mathbb{F}_{q^m}[\mathsf{x}]$. *Let* ψ *be the field isomorphism given in expression (1). Then, the determinant of the following polynomial matrix*

$$\psi(v_0) + \psi(v_1) + \psi(v_2)\mathbf{X} + \psi(v_3)\mathbf{X}^2 + \cdots + \psi(v_{r-1})\mathbf{X}^{r-2} + \mathbf{X}^{r-1}$$

is a primitive polynomial of degree rm *in* $\mathbb{F}_q[x]$.

PROOF: Given a square matrix M, given by

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix},$$

the determinant of M is $\det(M) = \det(C)\det(B - AC^{-1}D)$ as long as C is square and non-singular (Schur complement). According to Theorem 3.1, the characteristic polynomial of the matrix $\Psi(\mathbf{V})$ is a primitive polynomial, that is, the determinant of the polynomial matrix $\mathsf{x}I - \Psi(\mathbf{V})$ is a primitive polynomial. Now, we can divide that polynomial matrix into blocks as follows

$$\left[\begin{array}{ccccc|c} \mathbf{X} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & \psi(v_0) \\ \hline -\mathbf{I}_m & \mathbf{X} & \mathbf{O} & \cdots & \mathbf{O} & \psi(v_1) \\ \mathbf{O} & -\mathbf{I}_m & \mathbf{X} & \cdots & \mathbf{O} & \psi(v_2) \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{X} & \psi(v_{r-2}) \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \cdots & -\mathbf{I}_m & \mathbf{X} + \psi(v_{r-1}) \end{array}\right],$$

where $\mathbf{X} = \mathsf{x}I$. If we denote by

$$\Delta = \begin{bmatrix} -\mathbf{I}_m & \mathbf{X} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & -\mathbf{I}_m & \mathbf{X} & \cdots & \mathbf{O} \\ \vdots & \vdots & \vdots & & \vdots \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{X} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \cdots & -\mathbf{I}_m \end{bmatrix},$$

then, Δ is a square matrix and $\det(\Delta) = 1$. At this point, according to the Schur complement we have

$$\begin{aligned} \det(\mathsf{x}I - \Psi(\mathbf{V})) &= \det(\Delta)\det\left(\psi(v_0) - \begin{bmatrix} \mathbf{X} & \mathbf{O} & \ldots & \mathbf{O} \end{bmatrix}\Delta^{-1}\begin{bmatrix} \psi(v_1) \\ \vdots \\ \psi(v_{m-1}) \end{bmatrix}\right) \\ &= \det(\psi(v_0) + \psi(v_1) + \psi(v_2)\mathbf{X} + \psi(v_3)\mathbf{X}^2 + \cdots + \psi(v_{r-1})\mathbf{X}^{r-2} + \mathbf{X}^{r-1}), \end{aligned}$$

which is a primitive polynomial over $\mathbb{F}_q$. □

4 Conclusions

Primitive polynomials have many practical applications in communications, cryptography, coding theory, etc. In this work, a simple construction of primitive polynomials is given. Given two primitive polynomials of degrees b and r over $\mathbb{F}_q$ and $\mathbb{F}_{q^b}$, respectively, we are able to construct another polynomial over $\mathbb{F}_q$ with degree rb, constructing a matrix ring isomorphism and using the companion matrices of both polynomials.

Funding

The work of the first author was supported by FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) with number of process 2015/07246-0. The second author was partially supported by grant MINECO MTM2015-69138-REDT.

References

[1] Menezes AJ, van Oorschot PC, Vanstone SA. Handbook of applied cryptography. Boca Raton, FL: CRC Press; 1996.

[2] Golomb SW. Shift register-sequences. Laguna Hill, California: Aegean Park Press; 1982.

[3] Coppersmith D, Krawczyk H, Mansour Y. The shrinking generator. In: Advances in cryptology – crypto '93. Vol. 773 of Lecture Notes in Computer Science; Springer-Verlag; 1993. p. 23–39.

[4] Meier W, Staffelbach O. The self-shrinking generator. In: Cachin C, Camenisch J, editors. Advances in cryptology – eurocrypt 1994. Vol. 950 of Lecture Notes in Computer Science; Springer-Verlag; 1994. p. 205–214.

[5] Kanso A. Modified self-shrinking generator. Computers and Electrical Engineering. 2010;36(1):993–1001.

[6] MacWilliams FJ, Sloane NJA. The theory of error-correcting codes. 6th ed. Amsterdam: North-Holland; 1988.

[7] Cardell SD, Climent JJ, Requena V. A construction of MDS array codes. WIT Transactions on Information and Communication Technologies. 2013;45:47–58.

[8] Barg A, Zémor G. MDS array codes with optimal rebuilding. In: Proceedings of the 2011 IEEE International Symposium on Information Theory (ISIT 2011); Jul. Saint Pettersburg: IEEE; 2011. p. 1240–1244.

[9] Beard JTB, Jr, West KI. Some primitive polynomials of the third kind. Mathematics of Computation. 1974; 28(128):1166–1167.

[10] Hansen T, Mullen GL. Primitive polynomials over finite fields. Mathematics of Computation. 1992; 59(200):639–643.

[11] Stahnke W. Primitive binary polynomials. Mathematics of Computation. 1973;27(124):977–980.

[12] Watson EJ. Primitive polynomials (mod 2). Mathematics of Computation. 1962;16:368–269.

[13] Zierler N, Brillhart J. On primitive trinomials (mod 2). Information and control. 1968;13(6):541–554.

[14] Cohen SD, Mills D. Primitive polynomials with first and second coefficients prescribed. Finite Fields and Their Applications. 2003;9:334–350.

[15] Fan S, Han W. Character sums over Galois rings and primitive polynomials over finite fields. Finite Fields and their Applications. 2004;10:36–52.

[16] Fan S, Han W. Primitive polynomial with three coefficients prescribed. Finite Fields and their Applications. 2004;10:506–521.

[17] Cohen SD. Primitive elements and polynomials: existence results. Vol. 141 of Lecture Notes in Pure and Appl. Math.; New York; 1996. p. 43–55.

[18] Fan SQ, Han WB. p-adic formal series and Cohen's problem. Glasgow Mathematical Journal. 2003;46(1):47–61.

[19] Lidl R, Niederreiter H. Introduction to finite fields and their applications. New York, NY: Cambridge University Press; 1986.

[20] Cardell S. D. Constructions of MDS codes over extension alphabets [dissertation]. Alicante, España: Departamento de Ciencia de la Computación e Inteligencia Artificial, Universidad de Alicante; 2012 (available at https://rua.ua.es/dspace/bitstream/10045/27320/1/Tesis_Diaz_Cardell.pdf).